DOCKET: CU-5118

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Fabien THOMAS et al.   )
)
SERIAL NO: 10/594,106   ) Group Art Unit:
)
FILED: September 25, 2006   ) Examiner:

TITLE: DEVICE AND METHOD FOR DETECTING AND PREVENTING
                INTRUSION INTO A COMPUTER NETWORK

AMENDED CLAIMS

1. (currently amended) A method for the detection and prevention of intrusions into a computer network with a firewall, ~~that includes a stage for~~ the method comprising:

detecting the connections at [[the]] a central point and before each branch of [[the]] said network, ~~a stage for~~

selective filtering of the said connections, where [[the]] said selective filtering stage includes firstly a stage for automatic recognition of the accessing protocol, independently of the communication port used by the said protocol, and secondly, after [[the]] said accessing protocol has been recognised automatically, a stage for verifying the conformity of each communication flowing in a given connection to the said protocol, to deliver a dynamic authorisation for communications resulting from normal operation of the protocol and to deliver a dynamic rejection for communications resulting from abnormal operation of the protocol,

~~characterised in that:~~

[[the]] wherein said check on conformity is performed layer by layer, by successive protocol analysis of each part of the data packet flowing in the connection corresponding to a given protocol, from the lowest protocol to the highest protocol, and

wherein, since each main connection enabled is able to induce one or more secondary connections, [[the]] said check on conformity detects the data necessary for opening [[the]] said secondary connections and attaches [[the]] said secondary connections to the authorisation for connection of [[the]] said main connection.

1

2. (currently amended) A method according to claim 1, ~~characterised in that~~ wherein, as long as the accessing protocol of a connection is not recognised, the data are accepted but not transmitted.

3. (currently amended) A method according to claim 2, ~~characterised in that~~ wherein, if the number of data packets accepted but not transmitted exceeds a certain threshold, or if the data are accepted but not transmitted for a time exceeding a certain threshold, then the connection is considered not to have been analysed.

4. (currently amended) A method according to ~~any of claims 2 and 3, characterised in that~~ claim 2, wherein if the data are accepted but not transmitted for a time exceeding a certain threshold, then the connection is considered not to have been analysed.

5. (currently amended) A method according to ~~any of claims 2 and 4, characterised in that~~ claim 2, wherein, when the accessing protocol of a connection is not automatically recognised, said step of checking on conformity of each communication flowing in a given connection to [[the]] said protocol is ~~replace~~ replaced by a step of generic checking of coherence of data packets.

6. (currently amended) A device for the detection and prevention of intrusions into a computer network, ~~including~~ comprising:
    a firewall,
    a resource for preventing intrusions by detection of the connections, directly incorporated into [[the]] said firewall at [[the]] a central point and before each branch of [[the]] said network, where [[the]] said resource for the prevention of intrusions includes a resource for selective filtering of [[the]] said connections by automatic recognition of the accessing protocol, independently of the communication port used by [[[the]] said protocol,
        ~~characterised in that~~
                [[the]] wherein said selective filtering resource includes at least one independent module for the analysis of at least one given communication protocol, and
                at least one of the independent modules includes:
                i.   unit for the automatic recognition of a given communication protocol,
                ii.   unit for verifying the conformity of the communication flowing in a

2

given connection to the said protocol,

       iii.   means for delivering a dynamic authorisation for communications resulting from normal operation of the protocol, and delivering a dynamic rejection for communications resulting from abnormal operation of the protocol, <u>and</u>

       iv.   means of transmission of a part of a data packet to an independent analysis module of a hierarchically higher protocol.

7. (currently amended) A device according to claim 6, ~~characterised in that~~ <u>wherein</u>, in addition to the independent module or modules for the analysis of a given communication protocol, [[it]] <u>the device</u> includes an independent generic module which attaches itself to the connections for which the protocol has been recognised by none of the other said independent modules.

8. (currently amended) A device according to ~~any of claims 6 and 7, characterised in that it~~ <u>claim 6, wherein the device</u> includes an interface for entry<u>,</u> by [[the]] <u>a</u> user<u>,</u> of the criteria that determine the filtering policy.

9. (currently amended) A device according to claim 8, ~~characterised in that the~~ <u>wherein,</u> said interface receives the criteria specified in natural language by the user.

10. (currently amended) A device according to claim 9, ~~characterised in that the~~ <u>wherein</u> said criteria specified in natural language include at least one protocol name.

11. (currently amended) A device according to ~~any of claims 8 to 10, characterised in that the~~ <u>claim 8, wherein</u> said interface allows the activation or deactivation of each of [[the]] said independent modules.

12. (currently amended) A device according to ~~any of claims 6 to 11, characterised in that it~~ <u>claim 6, wherein the device</u> includes a resource for statistical processing of the connection data, and a resource for storage of [[the]] said connection data and processed data.